Attorney Docket No.: 16222U-016100US

PATENT APPLICATION

CENTRALIZED ELECTRONIC COMMERCE CARD TRANSACTIONS

Inventor(s): Steve Davis, a citizen of The United States, residing at
800 Metro Center Boulevard
Foster City, CA 94404

Assignee: Visa U.S.A.
123 Mission Street
San Francisco, CA, 94105

Entity: Large

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 415-576-0200

CENTRALIZED ELECTRONIC COMMERCE CARD TRANSACTIONS

BACKGROUND OF THE INVENTION

[0001] Electronic commerce cards are frequently used by consumers to make purchases from merchants over the Internet. Electronic commerce cards include credit cards, debit cards, prepaid purchase cards, travel cards, or any other system that can be used instead of cash to purchase goods or services. One example of an authentication system enables a cardholder to associate a password or other identifying information with an electronic commerce card. To make a purchase online, the consumer must provide the password or other identifying information associated with the electronic commerce card. This ensures that the person possessing the electronic commerce card is actually authorized to use the electronic commerce card.

[0002] Once a consumer has been authenticated as an authorized cardholder, the electronic commerce card transaction can be completed by the merchant. Previously, authentication and transaction processing used a decentralized, distributed computing model to communicate messages between merchants, card associations, and authentication servers. In this approach, there is no centralized point for collecting data and monitoring system performance. Instead, each end point in the system, such as merchants, authentication servers, and card issuers, must be asked to collect data and monitor performance of their portion of the overall system.

[0003] This decentralized model makes it difficult for the electronic commerce card association, which is responsible for the entire system, to evaluate the system performance as a whole. Additionally, this lack of visibility of the entire system prevents the card association from spotting trends or patterns that would assist in understanding where and how to add new features. Furthermore, the decentralized model makes upgrades and migration difficult, as each end point must be able to communicate with its counterparts, regardless of the features or software versions supported. The decentralized model also increases support and service overhead, and decreases the fault tolerance of the system.

[0004] Therefore, it is desirable to have an electronic commerce card authentication and transaction processing system that facilitates monitoring and management, increases overall reliability and fault tolerance, and simplifies system upgrades and migrations.

BRIEF SUMMARY OF THE INVENTION

[0005] An embodiment of the invention includes a central transaction server in electronic commerce card authorization system to enables the electronic commerce card association to manage and monitor the entire authentication system. The central transaction server acts as an intermediary for all communications to and from the access control server (ACS) used to authenticate a cardholder. Additionally, if any portion of the authentication system fails, for example, a card issuer's ACS, the central transaction server can compensate by providing appropriate responses to other portions of the system. Additionally, the centralized transaction server enables portions of the system to be upgraded without breaking compatibility with the non-upgraded portions. As all traffic between merchant and cardholder systems and the card issuer ACS systems is routed through the centralized transaction server, the centralized transaction server can translate all incoming traffic into a format compatible with the intended recipient.

[0006] In an embodiment, the central transaction server is adapted to receive an authentication request from a cardholder system, forward the authentication request to an access control server, and relay authentication information between the access control server and the cardholder system. The central authentication server also receives an authentication response from the access control server and forwards the authentication response to the cardholder system. The authentication response is adapted to be analyzed by a merchant system. In a further embodiment, the central transaction server is adapted to forward a copy of the authentication response to an authentication history server to be archived.

[0007] In an additional embodiment, the central transaction server is further adapted to receive a verifying enrollment request from a directory server, and to send a verifying enrollment response to the directory server. In one implementation, the central transaction server is adapted to send the verifying enrollment response in response to a query to the access control server. In an alternate implementation, the central transaction server is adapted to send the verifying enrollment response to the directory server without querying the access control server, and is further adapted to query the access control server in response to receiving an authentication request.

[0008] In another embodiment, the authentication request includes a pseudonym corresponding to an electronic commerce card account number and previously created by the

central transaction server. Alternately, the authentication request includes a pseudonym previously created by a merchant system that corresponds to an electronic commerce card account number.

[0009] In yet a further embodiment, the central transaction server is adapted to initiate a charge request via a card association network in response to receiving an authentication response from the access control server.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The invention will be described with reference to the drawings, in which:

Figure 1 illustrates a prior decentralized card authentication system;

Figure 2 illustrates an example card authentication system according to an embodiment of the invention; and

Figure 3 illustrates an example card authentication system according to an alternate embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0011] Figure 1 illustrates a prior decentralized card authentication system 100. System 100 enables cardholders to be authenticated when making electronic commerce card purchases online. Cardholder system 105 initiates an online purchase by accessing a merchant computer 110. In an embodiment, cardholder system 105 accesses a website provided by the merchant computer 110 via the Internet via a web browser. Alternatively, cardholder system 105 can access the merchant computer 110 via an alternate electronic communications network. The cardholder system 105 can be any type of communications device, for example a personal computer, a personal digital assistant, or a telephone.

[0012] To complete a purchase, a cardholder uses the cardholder system 105 to submit her electronic commerce card information 150, such as a card number and expiration date, to the merchant system 110. In an embodiment, a secure communication system, such as SSL, is used for all communications, including the electronic commerce card information 150.

[0013] In response to the electronic commerce card information 150, the merchant system initiates an authentication procedure to determine whether the electronic commerce card

information is valid and has been provided by an authorized cardholder. In an embodiment of system 100, there are numerous electronic commerce card issuers. Each electronic commerce card issuer is responsible for authenticating its own electronic commerce cards. To authenticate the electronic commerce card information 150, the merchant system 110 must locate the authentication service of the electronic commerce card issuer associated with the electronic commerce card information 150.

[0014] The merchant system sends a verifying enrollment request (VEReq) 152 to a directory server 120 to locate the appropriate authentication service. In an embodiment, all authentication-related communication is coordinated by an authentication plug-in 115 integrated with the merchant system 110. The VEReq 152 includes at least a portion of the electronic commerce card information 150 to be used by the directory server 120 to identify the authentication service associated with the cardholder's electronic commerce card. In an embodiment, each electronic commerce card issuer is assigned a different range of electronic commerce card numbers. This embodiment of the directory server 120 includes a list of all electronic commerce card issuers and their associated electronic commerce card number ranges. By comparing the electronic commerce card information with the list of electronic commerce card issuers, the directory server 120 is able to identify the appropriate authentication service.

[0015] After identifying the authentication service, the directory server 120 forwards the VEReq 154 to an access control server (ACS) 125 associated with the card issuer's authentication service. The ACS 125 determines whether the card information provided in the VEReq 154 can be authenticated. Card information may not be able to be authenticated by the ACS 125 if, for example, the card information does not include a valid electronic commerce card number, or if there is no authentication information associated with the electronic commerce card number.

[0016] If the electronic commerce card information provided in the VEReq 154 can be authenticated, the ACS 125 sends a verified enrollment response (VERes) 156 back to the directory server 120. The VERes 156 includes a message indicating that the ACS 125 can authenticate the electronic commerce card information and a pseudonym corresponding to the card number. The pseudonym can be any type of code or number that can be uniquely linked to card information by the ACS 125 at a later time. The VERes also includes a URL to be accessed by the cardholder system 105 to authenticate the cardholder. For system 100, the

URL is associated with a web site provided by the ACS 125. Upon receiving a VERes from the ACS 125, the directory server 120 forwards the VERes 158 to the merchant system 110.

[0017] From the received VERes, the merchant system 110 generates an authentication request. The authentication request includes the pseudonym created by the ACS 125 and transaction information associated with the cardholder's prospective purchase. The merchant system then forwards the authentication request 160 to the cardholder system 105. In an embodiment, the authentication request is sent to the cardholder system 105 with a web page having a redirection command, such as an HTTP redirect, to a web site hosted by the ACS 125. This web page also includes a URL for returning information to the merchant system 110.

[0018] In response the authentication request received from the merchant system 110, the cardholder system 105 accesses 162 a web site hosted by the ACS 125. In accessing this web site, the cardholder system 105 supplies the ACS 125 with the pseudonym originally created by the ACS for the VERes.

[0019] The cardholder to authenticates her identity by presenting authentication information 164 to the web site provided by the ACS 125. In an embodiment, the cardholder authenticates her identity by providing to the ACS 125 a password or other identifying information previously associated with the electronic commerce card. The ACS 125 uses the pseudonym provided by the cardholder system to identify the electronic commerce card being supplied by the cardholder and retrieve authentication information previously associated with the electronic commerce card. In an embodiment, the ACS 125 matches the pseudonym received via the authentication request 162 with the pseudonym previously created for VERes 156. In a further embodiment, the pseudonym expires after a limited period of time, for example five minutes, to prevent fraudulent reuse of the authentication request.

[0020] The ACS 125 returns an authentication response 166 to the cardholder system 105. The cardholder system 105 in turn forwards the authentication response 168 to the merchant system 110. If the authentication information 164 provided by the cardholder matches the authentication information previously associated with the electronic commerce card, the authentication response includes a message indicating that the authentication was successful. Alternatively, the authentication response can include a message indicating that the authentication failed. In a further embodiment, the authentication response also includes an error code identifying the reason for authentication failure.

[0021] In addition to sending the authentication response to the merchant system 110, a copy of the authentication response 167 is sent to an authentication history server 135. The authentication history server 135 maintains an archive of all authentications performed by the system 100. The authentication response is digitally signed to prevent the cardholder system 105 or other third party systems from tampering with the contents of the authentication response.

[0022] After receiving the authentication response 168, the merchant system 110 validates the authentication response. To validate the authentication response 168, the merchant system 110 first verifies the digital signature associated with the authentication response to ensure that there has not been any tampering. Once the authentication response is determined to have arrived intact, and the response is for the request originally submitted, the contents of the authentication response are analyzed to determine if authentication has been successful. If the authentication was not successful, the merchant system 110 halts the transaction. If the authentication was successful, the merchant system 110 can continue with the transaction by initiating a charge to the electronic commerce card provided by the cardholder. In an embodiment, the merchant system 110 charges the electronic commerce card by submitting the card information to a card acquirer 144. The card acquirer then sends the charge request over a private card association network 148 to be processed by the electronic commerce card issuer associated with the card. In a further embodiment, an electronic commerce indicator and a Cardholder Authentication Verification Value, which indicates that the electronic commerce card has been successfully verified, is included with the charge request.

[0023] The decentralized nature of the electronic commerce card authentication system 100 makes it difficult to be managed and monitored by electronic commerce card associations. Additionally, if any portion of the system 100 fails, for example, a card issuer's ACS, there is no way for the system 100 to compensate. The decentralized electronic commerce card authentication system 100 is difficult to upgrade, as each end point of the system, for example the directory server and the numerous ACS and merchant systems, must all be upgraded simultaneously to ensure compatibility.

[0024] Figure 2 illustrates an example improved card authentication system 200 according to an embodiment of the invention. Cardholder system 205 initiates an online purchase by accessing a merchant computer 210. In an embodiment, cardholder system 205 accesses a website provided by the merchant computer 210 via the Internet using a web browser.

Alternatively, cardholder system 205 can access the merchant computer 210 via an alternate electronic communications network. The cardholder system 205 can be any type of communications device, for example a personal computer, a personal digital assistant, or a telephone.

[0025] To complete a purchase, a cardholder uses the cardholder system 205 to submit her electronic commerce card information 250, such as a card number and expiration date, to the merchant system 210. In an embodiment, a secure communication system, such as SSL, is used for all communications, including the electronic commerce card information 250.

[0026] In response to the electronic commerce card information 250, the merchant system initiates an authentication procedure to determine whether the electronic commerce card information is valid and has been provided by an authorized cardholder. To authenticate the electronic commerce card information 250, the merchant system 210 must locate the authentication service of the electronic commerce card issuer associated with the electronic commerce card information 250.

[0027] The merchant system sends a verifying enrollment request (VEReq) 252 to a directory server 220 to locate the appropriate authentication service. In an embodiment, all authentication-related communication is coordinated by an authentication plug-in 215 integrated with the merchant system 210. The VEReq 252 includes at least a portion of the electronic commerce card information 250 to be used by the directory server 220 to identify the access control server (ACS) 225 associated with the cardholder's electronic commerce card. In an embodiment, each electronic commerce card issuer is assigned a different range of electronic commerce card numbers. This embodiment of the directory server 220 includes a list of all electronic commerce card issuers and their associated electronic commerce card number ranges. By comparing the electronic commerce card information with the list of electronic commerce card issuers, the directory server 220 is able to identify the appropriate ACS.

[0028] After identifying the ACS, the directory server 220 forwards the VEReq 272 to a central transaction server 280. As discussed in detail below, the central transaction server 280 acts as a proxy for all communications between ACS systems and cardholder systems, merchant systems, authentication history servers, and directory servers. In response to the VEReq 272, the central transaction server 280 replies with a VERes 274. In this embodiment, the central transaction server 280 creates a VERes 274 without checking with

the ACS 225 to determine whether the card information can be authenticated. This is done for compatibility purposes, and, as discussed below, streamlines the authentication process.

[0029] In an alternate embodiment, the central transaction server 280 forwards the VEReq to the ACS 225. ACS 225 returns a VERes, similar to that discussed above, to the central transaction server 280. The central transaction server 280 alters the VERes received from the ACS 225 to direct the cardholder system 205 to include a URL is associated with a web site provided by the central transaction server 280, as discussed in detail below, rather than a web site provided by the ACS, as discussed in system 100. If the ACS 225 is not available, or an error is encountered while communicating with the ACS 225, or if the response from the ACS 225 cannot be understood, the central transaction server 280 will generate a substitute VERes on behalf of the ACS, including an indication of why the response is being generated. Examples of these indicators include: 1) the cardholder has not provided authentication information; 2) the card issuer has not implemented the authentication system; 3) the central transaction server 280 timed out waiting on a response from the ACS 225; and 4) the VERes received from ACS 225 could not be understood by the central transaction server 280. The indicator in included in the pseudonym associated with the card information and is used later in generating the Cardholder Authentication Verification Value.

[0030] The VERes 274 created by the central transaction server 280 includes a message indicating that the ACS 225 can authenticate the electronic commerce card information and a pseudonym corresponding to the card number. The pseudonym can be any type of code or number that can be uniquely linked to card information by the ACS 225 at a later time. The VERes also includes a URL to be accessed by the cardholder system 205 to authenticate the cardholder. For system 200, the URL is associated with a web site provided by the central transaction server 280. Upon receiving a VERes from the central transaction server 280, the directory server 220 forwards the VERes 258 to the merchant system 210.

[0031] From the received VERes, the merchant system 210 generates an authentication request. The authentication request includes the pseudonym created by the central transaction server 280 and transaction information associated with the cardholder's prospective purchase. The merchant system then forwards the authentication request 260 to the cardholder system 205. In an embodiment, the authentication request is sent to the cardholder system 205 with a web page having a redirection command, such as an HTTP

redirect, to a web site hosted by the central transaction server 280. This web page also includes a URL for returning information to the merchant system 210.

[0032] In response the authentication request received from the merchant system 210, the cardholder system 205 accesses 262 the web site hosted by the central transaction server 280. In accessing this web site, the cardholder system 205 supplies the central transaction server 280 with the authentication request, including the pseudonym created by the central transaction server 280 earlier.

[0033] The central transaction server 280 provides a VEReq 254 to the ACS 225 associated with the card issuer's authentication service. The ACS 225 determines whether the card information provided in the VEReq 254 can be authenticated. If the electronic commerce card information provided in the VEReq 254 can be authenticated, the ACS 225 sends a verified enrollment response (VERes) 256 back to the central transaction server. In this embodiment, the central transaction server 280 has integrated the step of sending a VEReq and receiving a VERes into the processing of authentication request from the cardholder system, which streamlines the authentication process. As discussed above, an alternate embodiment of the central transaction server 280 previously sent a VEReq to the ACS 225, and thus does not need to repeat this communication.

[0034] In response to the VERes 256, the central transaction server 280 sends the authentication request received from the merchant system 210 via the cardholder system 205 to the ACS 225. The cardholder authenticates her identity by presenting authentication information to the web site provided by the ACS 225. The central transactions server relays all communications 276 between the cardholder system 205 and the ACS 225. In an alternate embodiment, communications 276 between the cardholder system and the ACS 225 occur directly without the central transaction server as an intermediary.

[0035] In an embodiment, the cardholder authenticates her identity by providing to the ACS 225 a password or other identifying information previously associated with the electronic commerce card. The ACS 225 uses the pseudonym provided by the cardholder system to identify the electronic commerce card being supplied by the cardholder and retrieve authentication information previously associated with the electronic commerce card. In an embodiment, the ACS 225 matches the pseudonym received via the authentication request with the pseudonym previously created for VERes 156. In a further embodiment, the pseudonym expires after a limited period of time, for example five minutes, to prevent

fraudulent reuse of the authentication request. In another embodiment, the ACS 225 and the central transaction server 280 each generate their own unique pseudonym corresponding to the electronic commerce card. By allowing the ACS 225 to generate and use its own pseudonym to identify the electronic commerce card, the ACS 225 does not need to be changed to work with the central transaction server 280.

[0036] The ACS 225 returns an authentication response 266 to the central transaction server 280, which in turn forwards an authentication response 278 to the cardholder system 205. The cardholder system 205 in turn forwards the authentication response 268 back to the merchant system 210. If the authentication information 164 provided by the cardholder matches the authentication information previously associated with the electronic commerce card, the authentication response includes a message indicating that the authentication was successful. Alternatively, the authentication response can include a message indicating that the authentication failed. In a further embodiment, the authentication response also includes an error code identifying the reason for authentication failure.

[0037] If, for example, the ACS 225 does not support authentication functions, the ACS 225 is not operating or does not reply to the central transaction server 280 within a predetermined period of time, or the central transaction server 280 does not understand the VERes provided by the ACS 225, the ACS 225 cannot authenticate the electronic commerce card information. In response to an authentication failure by the ACS, for these example reasons or any other reason, an embodiment of the central transaction server 280 can return an attempted authentication response to the cardholder system 205. The attempted authentication response can authorize the merchant system 210 to continue the transaction without authentication, or to halt the transaction. The action specified by the attempted authentication response can be determined by one or more business rules, for example, permitting a transaction to continue without authorization if the ACS is unavailable, but halting the transaction if the ACS returns an unintelligible VERes.

[0038] In addition to sending the authentication response to the merchant system 210, a copy of the authentication response 267 is sent from the ACS 225 to an authentication history server 235 via the central transaction server 280. The authentication history server 235 maintains an archive of all authentications performed by the system 200.

[0039] After receiving the authentication response 268, the merchant system 210 validates the authentication response. The authentication response is digitally signed to prevent the

cardholder system 205 or other third party systems from tampering with the contents of the authentication response.

[0040] To validate the authentication response 268, the merchant system 210 first verifies the digital signature associated with the authentication response to ensure that there has not been any tampering. Once the authentication response is determined to have arrived intact, and the response is for the request originally submitted, the contents of the authentication response are analyzed to determine if authentication has been successful. If the authentication was not successful, the merchant system 210 halts the transaction. If the authentication was successful, the merchant system 210 can continue with the transaction by initiating a charge to the electronic commerce card provided by the cardholder. In an embodiment, the merchant system 210 charges the electronic commerce card by submitting the card information to a card acquirer 244. The card acquirer then sends the charge request over a private card association network 248 to be processed by the electronic commerce card issuer associated with the card. In a further embodiment, an electronic commerce indicator and a Cardholder Authentication Verification Value, which indicates that the electronic commerce card has been successfully verified, is included with the charge request.

[0041] The use of a central transaction server in system 200 enables the electronic commerce card association to managed and monitored the entire authentication system easily. Additionally, if any portion of the system 200 fails, for example, a card issuer's ACS, the central transaction server can compensate by providing appropriate responses to other portions of the system. Additionally, the centralized transaction server enables portions of the system to be upgraded without breaking compatibility with the non-upgraded portions. As all traffic between merchant and cardholder systems and the card issuer ACS systems is routed through the centralized transaction server, the centralized transaction server can translate all incoming traffic into a format compatible with the intended recipient.

[0042] An additional advantage of the centralized transaction server is that it enables the integration of formally separate portions of the authentication system into a single unit. This integration increases reliability, decreases service overhead, and allows for streamlining of the authentication process.

[0043] Figure 3 illustrates an example card authentication system 300 according to an alternate embodiment of the invention. In this embodiment, the functions of the directory server and the authentication history server have been integrated into the central transaction

server and the card association network, enabling the elimination of several steps of the authentication process. As with other embodiments, cardholder system 305 initiates an online purchase by accessing a merchant computer 310. To complete a purchase, a cardholder uses the cardholder system 305 to submit her electronic commerce card information 350 to the merchant system 310.

[0044] In response to the electronic commerce card information 350, the merchant system 310 initiates an authentication procedure to determine whether the electronic commerce card information is valid and has been provided by an authorized cardholder. To authenticate the electronic commerce card information 350, the merchant system 310 sends an authentication request 352 to the cardholder system 305. The authentication request includes a pseudonym created by the merchant system 310 and transaction information associated with the cardholder's prospective purchase. The pseudonym can be any type of code or number that can be uniquely linked to card information by the central transaction server 380 at a later time.

[0045] In an embodiment, the authentication request is sent to the cardholder system 305 with a web page having a redirection command, such as an HTTP redirect, to a web site hosted by the central transaction server 380. This web page also includes a URL for returning information to the merchant system 310.

[0046] In response the authentication request received from the merchant system 310, the cardholder system 305 accesses 354 the web site hosted by the central transaction server 380. In accessing this web site, the cardholder system 305 supplies the central transaction server 380 with the authentication request, including the pseudonym created by the merchant system 310. The central transaction server 380 determines the card information from the pseudonym provided in the authentication request. The card information is then used by the central transaction server 380 to identify the ACS 325 responsible for authenticating the cardholder, for example by comparing the electronic commerce card information with the electronic commerce card number ranges associated with card issuers.

[0047] The central transaction server 380 sends a verifying enrollment request (VEReq) 358 to the appropriate ACS 325 to confirm that the ACS can authenticate the card information provided. A copy 356 of the VEReq is sent to the card association network 348 for archival. If the ACS 325 responds with a successful VERes, the central transaction server 380 then facilitates the exchange of authentication information 360 between the cardholder

system 305 and the ACS 325. Upon successful authentication, the ACS 325 sends an authentication response 362 to the central transaction server 380. The central transaction server 380 in turns forwards a copy 366 of the authentication response to the cardholder system 305 and another copy 364 of the authentication response to the card association network 348 for archival.

[0048] The cardholder system 305 forwards a copy of the authentication response 368 back to the merchant system 310. After receiving the authentication response 368, the merchant system 310 validates the authentication response by verifying the digital signature associated with the authentication response to ensure that there has not been any tampering and analyzing the authentication response. If the authentication was not successful, the merchant system 310 halts the transaction. If the authentication was successful, the merchant system 310 can continue with the transaction by initiating a charge to the electronic commerce card provided by the cardholder. In an embodiment, the merchant system 310 charges the electronic commerce card by submitting the card information to a card acquirer 344. The card acquirer then sends the charge request 370 over a private card association network 348 to be processed by the electronic commerce card issuer associated with the card.

[0049] As the different portions of authentication system are integrated into the central transaction server 380, additionally optimizations can be implemented. For example, in a further embodiment, the central transaction server 380 initiates a charge to the electronic commerce card automatically when the ACS 325 returns a successful authentication response. In this embodiment, the acquirer 344 is bypassed and the central transactions server 380 sends the charge request directly to the card association network 348.

[0050] Although the invention has been discussed with respect to specific embodiments thereof, these embodiments are merely illustrative, and not restrictive, of the invention. For example, the present invention can be utilized with any authentication system. Thus, the scope of the invention is to be determined solely by the claims.